Sub a2 5

1. A method of digitally signing a message exchanged between a pair of correspondents in a data transmission system, said method comprising the steps of subdividing said message into a pair of bit strings, utilising one of said bit strings to compute a first signature component, forming from said first signature component and another of said bit strings an intermediate signature component, utilising said intermediate component to provide a second signature component and combining said first and second components with said other of said bit strings to provide a signature.
2. A method according to claim 1 wherein redundancy in said one of said bit strings is compared to a predetermined level prior to computing said first signature component.
3. A method according to claim 2 wherein said redundancy is adjusted to exceed said predetermined level.
4. A method according to claim 3 wherein data is added to said one bit string to adjust said redundancy.
5. A method according to claim 4 wherein an indicator is included in said one bit string to indicate the data added.
6. A method according to claim 1 wherein said second component is generated by hashing said first component and said other bit string.
7. A method of verifying a message subdivided into a pair of bit strings from a signature including at least one component having only one of said bit strings encrypted therein, and the other of said bit strings, said method comprising the steps of combining said one component with the other bit string, recovering said one bit string from said combination using publicly available information of the purported signer and examining said recovered one bit string for a predetermined characteristic.
8. A method according to claim 7 wherein said combination of said one component and said other bit string includes hashing a combination of said one component and said other bit string.
9. A method according to claim 8 wherein said predetermined characteristic is the redundancy of said recovered one bit string.

10. A method according to claim 9 wherein said signature includes a second component derived from a combination of said one component and said other bit string and said one bit string is recovered utilising said second component.